Claims

What is claimed is:

Sub A1

1. A method for validating a packet in a computer network, comprising the steps of:

deriving a session key for said packet;

selecting at least one of a plurality of security policies as a function of the session key; and

using the selected at least one of the security policies in validating said packet.

2. The method of claim 1 wherein the session key includes items derived from header information appended to data in said packet.

3. The method of claim 1 wherein the session key includes at least one item from the set consisting of (i) a source address, (ii) a destination address, (iii) a next-level protocol, (iv) a source port associated with a protocol, and (v) a destination port associated with the protocol.

4. The method of claim 1 wherein the session key includes at least one item from the set consisting of (i) an Internet protocol (IP) source address, (ii) an IP destination address, (iii) a next-level protocol, (iv) the source port associated with the protocol, and (v) the destination port associated with the protocol.

5. The method of claim 3 wherein the next-level protocol is transmission control protocol (TCP) or universal datagram protocol (UDP).

6. The method of claim 1 wherein the network includes a plurality of network interfaces, and wherein the selecting step comprises the step of determining the interface at which the request was received.

Sub A1 >

7. The method of claim 1 wherein the network includes a plurality of network interfaces, and wherein the selecting step comprises the step of determining the interface to which the request is to be sent.

8. A method for validating a packet in a computer network, comprising the steps of:

designating a plurality of independent security policies, with each of the security policies including a set of access rules;

determining which security policy is appropriate for the packet; and

validating the packet using the set of access rules of the determined security policy.

9. The method of claim 8 wherein at least a subset of the security policies correspond to different groups associated with a single firewall.

10. The method of claim 8 wherein at least a subset of the security policies correspond to different sub-groups within a given group.

11. The method of claim 8 wherein only an administrator for a given group has access to modify rules of a security policy for that group.

12. An apparatus for use in validating a packet in a firewall of a computer network, the firewall designating a plurality of independent security policies, with each of the security policies including a set of access rules, the apparatus comprising:

a processor associated with the firewall and operative (i) to process the packet to determine which of the security policies is appropriate for the packet, and (ii) to validate the packet using the set of access rules of the determined security policy.

Sub A1

13. The apparatus of claim 12 wherein at least a subset of the security policies correspond to different groups associated with a single firewall.

14. The apparatus of claim 12 wherein at least a subset of the security policies correspond to different sub-groups within a given group.

15. The apparatus of claim 12 wherein only an administrator for a given group has access to modify rules of a security policy for that group.

16. A method of providing a firewall in a computer network, comprising the steps of:

segmenting access rules into a plurality of domains; and

administering the access rules such that only an administrator for a given domain is permitted to modify rules of a security policy for that domain.

17. A computer system for packet validation in a computer network, comprising:

means for obtaining at least one data item from a request for a session;

means for selecting at least one of a plurality of security policies as a function of the data item; and

means for using the selected at least one of the security policies in validating packets of the session.

18. The computer system of claim 17 wherein the network includes a plurality of network interfaces, and wherein the means for selecting comprises means for determining the interface at which the request was received.

19. The computer system of claim 18 wherein the means for determining comprises means for referring to a source IP address contained in the request.

Sub A1

20. The computer system of claim 17 wherein the network includes a plurality of network interfaces, and wherein the means for selecting comprises means for determining the interface to which the request is to be sent.

21. The computer system of claim 20 wherein the means for determining comprises means for referring to a destination IP address contained in the request.

22. A method for packet validation in a computer network, comprising the steps of:

obtaining at least one data item from a request for a session;

selecting at least one of a plurality of security policies as a function of the data item; and

using the selected at least one of the security policies in validating packets of the session.

23. The method of claim 22 wherein the network includes a plurality of network interfaces, and the selecting step includes determining the interface at which the request was received.

24. The method of claim 23 wherein the determining step includes referring to a source IP address contained in the request.

25. The method of claim 22 wherein the network includes a plurality of network interfaces, and the selecting step includes determining the interface to which the request is to be sent.

26. The method of claim 25 wherein the determining step includes referring to a destination IP address contained in the request.